



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Adobe**

Tracking #:432317081

Date:15-04-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Adobe has released security updates to address multiple vulnerabilities in its products.

## TECHNICAL DETAILS:

Adobe has released security updates to address multiple vulnerabilities in ColdFusion, including 11 critical-severity flaws. These vulnerabilities could allow attackers to perform arbitrary file reads, execute code, bypass security features, and compromise affected systems.

### Adobe ColdFusion Vulnerabilities:

- **CVE-2025-24446** (CVSS score: 9.1): Improper input validation leading to arbitrary file system read.
- **CVE-2025-24447** (CVSS score: 9.1): Deserialization of untrusted data leading to arbitrary code execution.
- **CVE-2025-30281** (CVSS score: 9.1): Improper access control leading to arbitrary file system read.
- **CVE-2025-30282** (CVSS score: 9.1): Improper authentication leading to arbitrary code execution.
- **CVE-2025-30284** (CVSS score: 8.0): Deserialization of untrusted data leading to arbitrary code execution.
- **CVE-2025-30285** (CVSS score: 8.0): Deserialization of untrusted data leading to arbitrary code execution.
- **CVE-2025-30286** (CVSS score: 8.0): Operating system command injection leading to arbitrary code execution.
- **CVE-2025-30287** (CVSS score: 8.1): Improper authentication leading to arbitrary code execution.
- **CVE-2025-30288** (CVSS score: 7.8): Improper access control leading to a security feature bypass.
- **CVE-2025-30289** (CVSS score: 7.5): Operating system command injection leading to arbitrary code execution.
- **CVE-2025-30290** (CVSS score: 8.7): Path traversal leading to a security feature bypass.

Adobe has addressed these ColdFusion vulnerabilities in the following updates:

- **ColdFusion 2021 Update 19**
- **ColdFusion 2023 Update 13**
- **ColdFusion 2025 Update 1**

### Other Adobe Product Updates:

Security fixes have also been released for several other Adobe applications to resolve out-of-bounds write and heap-based buffer overflow bugs that could result in arbitrary code execution. These include:

- **After Effects:** CVE-2025-27182, CVE-2025-27183
- **Media Encoder:** CVE-2025-27194, CVE-2025-27195
- **Bridge:** CVE-2025-27193
- **Premiere Pro:** CVE-2025-27196
- **Photoshop:** CVE-2025-27198
- **Animate:** CVE-2025-27199



- **FrameMaker:** CVE-2025-30304, CVE-2025-30297, CVE-2025-30295

**Note:** Refer to Adobe's security bulletins for details on affected and fixed versions, as well as additional information.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Adobe.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- <https://helpx.adobe.com/security/security-bulletin.html>